CLAIMS

What is claimed is:

1. A method comprising:

receiving a network packet having a corresponding security association (SA);

determining for the packet a key value corresponding to the SA;

using the key value to determine a location of an entry in a lookup table, the entry containing information corresponding to the SA;

retrieving from the entry an index to a location of the SA in memory; and

retrieving the SA from memory based on the index.

2. The method of claim 1 wherein receiving a network packet comprises a device driver being passed an egress packet from an electronic system operating system.

3. The method of claim 1 wherein receiving a network packet comprises a device driver being passed an ingress packet from a network interface device.

4. The method of claim 1 wherein the key value is a handle created for the SA for an egress packet.

5. The method of claim 1 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

6. The method of claim 1 wherein the lookup table entry comprises the key value and the index.

7. The method of claim 6 wherein the lookup table entry further comprises a counter to track collisions for the entry.

8. The method of claim 1 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table.

9. The method of claim 1 further comprising an entry containing information for an SA corresponding to egress traffic being in a first lookup table, and an entry containing information for an SA corresponding to ingress traffic being in a second lookup table.

10. The method of claim 1 further comprising supporting a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

11. The method of claim 1 wherein the key value is determined by using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

12. An article comprising a machine-accessible medium to provide content to cause one or more electronic systems to:

receive a network packet having a corresponding security association (SA);

determine for the packet a key value corresponding to the SA;

use the key value to determine a location of an entry in a lookup table, the entry containing information corresponding to the SA;

retrieve from the entry an index to a location of the SA in memory; and

retrieve the SA from memory based on the index.

13. The article of claim 12 wherein to receive a network packet comprises a device driver to be passed an egress packet from an electronic system operating system.

14. The article of claim 12 wherein to receive a network packet comprises a device driver to be passed an ingress packet from a network interface device.

15. The article of claim 12 wherein the key value is a handle created for the SA for an egress packet.

16. The article of claim 12 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

17. The article of claim 12 wherein the lookup table entry comprises the key value and the index.

18. The article of claim 17 wherein the lookup table entry further comprises a counter to track collisions for the entry.

19. The article of claim 12 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table.

20. The article of claim 12 further comprising an entry containing information for an SA corresponding to egress traffic being in a first lookup table, and an entry containing information for an SA corresponding to ingress traffic being in a second lookup table.

21. The article of claim 12 further comprising to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

22. The article of claim 12 wherein the key value is to be determined by using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

23. An electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising content to cause one or more electronic systems to:

receive a network packet having a corresponding security association (SA);

determine for the packet a key value corresponding to the SA;

use the key value to determine a location of an entry in a lookup table, the entry containing information corresponding to the SA;

retrieve from the entry an index to a location of the SA in memory; and

retrieve the SA from memory based on the index.

24. The electronic data signal of claim 23 wherein to receive a network packet comprises a device driver to be passed an egress packet from an electronic system operating system.

25. The electronic data signal of claim 23 wherein to receive a network packet comprises a device driver to be passed an ingress packet from a network interface device.

26. The electronic data signal of claim 23 wherein the key value is a handle created for the SA for an egress packet.

27. The electronic data signal of claim 23 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

28. The electronic data signal of claim 23 wherein the lookup table entry comprises the key value and the index.

29. The electronic data signal of claim 28 wherein the lookup table entry further comprises a counter to track collisions for the entry.

30. The electronic data signal of claim 23 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table.

31. The electronic data signal of claim 23 further comprising an entry containing information for an SA corresponding to egress traffic being in a first lookup table, and an entry containing information for an SA corresponding to ingress traffic being in a second lookup table.

32. The electronic data signal of claim 23 further comprising to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

33. The electronic data signal of claim 23 wherein the key value is to be determined by using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

34. An electronic system comprising:

one or more processors;

a network interface coupled with the one or more processors to provide a communications path between the electronic system and a network; and

a memory coupled with the one or more processors, the memory to have a program to receive a network packet having a corresponding security association (SA), the program to determine for the packet a key value corresponding to the SA, to use the key value to determine a location of an entry in a lookup table, the entry containing information corresponding to the SA, to retrieve from the entry an index to a location of the SA in memory, and to retrieve the SA from memory based on the index.

35. The electronic system of claim 34 wherein the program to receive a network packet comprises a device driver corresponding to the network interface, the device driver to be passed an egress packet from an operating system.

36. The electronic system of claim 34 wherein the program to receive a network packet comprises a device driver corresponding to the network interface, the device driver to be passed an ingress packet from the network interface.

37. The electronic system of claim 34 wherein the key value is a handle created for the SA for an egress packet.

38. The electronic system of claim 34 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

39. The electronic system of claim 34 wherein the lookup table entry comprises the key value and the index.

40. The electronic system of claim 39 wherein the lookup table entry further comprises a counter to track collisions for the entry.

41. The electronic system of claim 34 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table.

42. The electronic system of claim 34 further comprising an entry containing information for an SA corresponding to egress traffic being in a first lookup table, and an entry containing information for an SA corresponding to ingress traffic being in a second lookup table.

43. The electronic system of claim 34 further comprising the program to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

44. The electronic system of claim 34 wherein to hash the key value is to be determined by using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.